Listing of Claims

1. (original) A cryptography accelerator for generating a stream cipher, the cryptography accelerator comprising:

a key stream generation core for performing key stream generation operations;

a memory associated with the key stream generation core, the memory including a plurality of input ports configured to obtain write data associated with a stream cipher and a plurality of output ports configured to provide read data associated with the stream cipher, wherein the key stream generation core and the memory are operable for performing a plurality of read data operations and a plurality of write data operations associated with generating the stream cipher in a single cycle.

2. (original) The cryptography accelerator of claim 1, wherein generation of the stream cipher is pipelined using coherency checking.

3. (original) The cryptography accelerator of claim 1, wherein the coherency checking comprises determining whether a write address is the same as a read address in a single cycle.

4. (original) The cryptography accelerator of claim 3, wherein a read operation bypasses the memory when the write address is the same as the read address.

5. (original) The cryptography accelerator of claim 1, wherein the stream cipher is associated with three variables.

6. (original) The cryptography accelerator of claim 5, wherein a read operation and a write operation are performed using a first variable and the memory in a first cycle.

7. (original) The cryptography accelerator of claim 6, wherein a read operation and a write operation are performed using a second variable and the memory in a second cycle.

8. (original) The cryptography accelerator of claim 7, wherein a read operation and a write operation are performed using a third variable and the memory in a third cycle.

9. (original) The cryptography accelerator of claim 1, wherein the stream cipher is ARC4.

10. (original) The cryptography accelerator of claim 1, wherein the memory is initialized in a single cycle.

11. (original) The cryptography accelerator of claim 1, further comprising a plurality of byte flops.

12. (original) The cryptography accelerator of claim 1, wherein the key stream generation core is operable to perform key shuffle operations and key stream generation operations.

13. (previously presented) A memory associated with a cryptography engine for generating a stream cipher, the memory comprising:

a plurality of input ports configured to obtain write data associated with generating a stream cipher;

a plurality of output ports configured to provide read data associated with the stream cipher, wherein a plurality of read data operations and the plurality of write data operations associated with generating the stream cipher are performed in a single cycle.

14. (original) The memory of claim 13, wherein the stream cipher can be performed in pipelined fashion using coherency checking.

15. (original) The memory of claim 13, wherein the coherency checking comprises determining whether a write address is the same as a read address in a single cycle.

16. (original) The memory of claim 15, wherein a read operation bypasses the memory when the write address is the same as the read address.

17. (original) The memory of claim 13, wherein the stream cipher is associated with three variables.

18. (original) The memory of claim 17, wherein a read operation and a write operation are performed using a first variable and the memory in a first cycle.

19. (original) The memory of claim 18, wherein a read operation and a write operation are performed using a second variable and the memory in a second cycle.

20. (original) The memory of claim 19, wherein a read operation and a write operation are performed using a third variable and the memory in a third cycle.

21. (original) The memory of claim 13, wherein the stream cipher is ARC4.

22. (original) The memory of claim 13, wherein the memory is initialized in a single cycle.

23. (original) The memory of claim 13, further comprising a plurality of byte flops.